

IX JORNADAS STIC CCN-CERT

DETECCIÓN E INTERCAMBIO, FACTORES CLAVE

Madrid, 10 y 11 de diciembre 2015

INTERCAMBIO DE INFORMACION CON REYES



- Reinoso Guzmán
- Innotec System - Entelgy
- reinoso_guzman@innotecsystem.com

Está basado en la tecnología

Malware

Information

Sharing

Platform



**Repositorio común
Y Estructurado
de amenazas
y código dañino**



Fuentes de malware

Fuentes:



Piloto:



Castilla-La Mancha

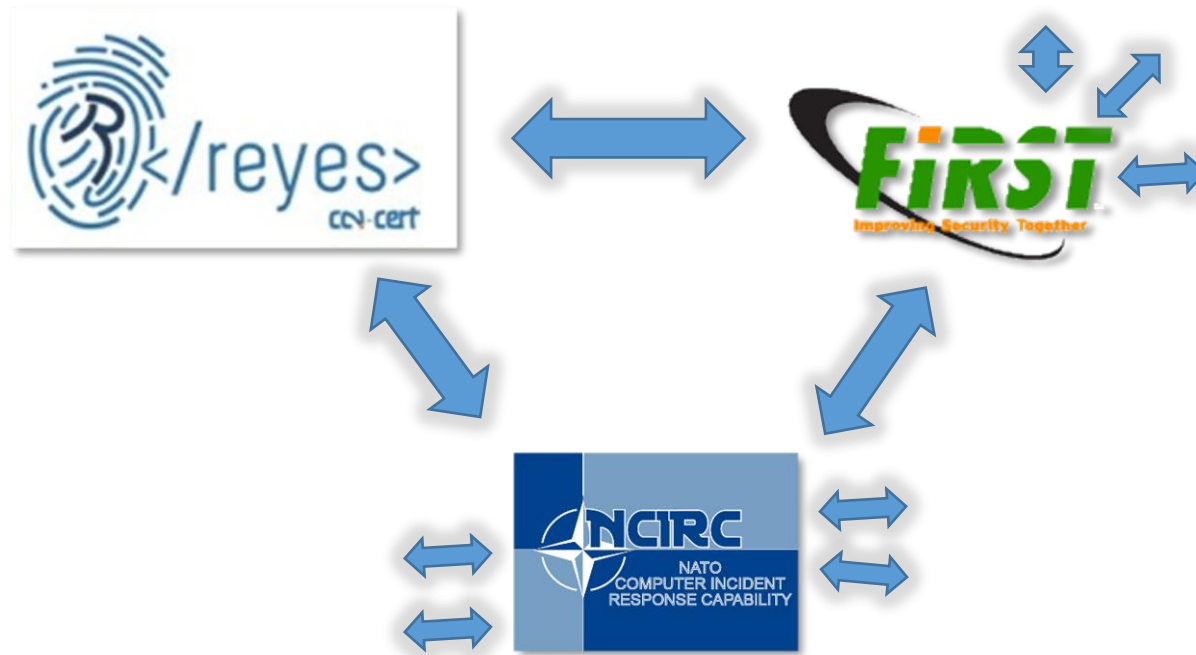


Junta de Castilla y León



Información e incidentes

Federación inter-MISP



Integración y realimentación



carmen



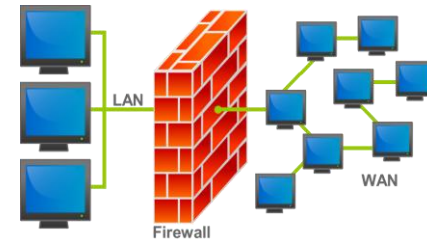
LUCIA

Estructurado





Exportación



Estadísticas piloto

2.600 eventos

70 organizaciones

445.000 atributos

1	97.812	hashes (md5, sha1, sha256)
	65.246	IP sospechosas
	45.836	URL
	32.887	Dominios malware
	16.596	Reglas Snort
	5.694	Vulnerabilidades asociadas
	1.186	Claves de registro
	585	Reglas yara

✓	Panda	Panda	30761	Panda	14	panda@ccn-cert.cni.es	2015-12-01	Medium	Completed	Trojan-Dropper.Win32.Injector
✓	Panda	Panda	30760	Panda	23	panda@ccn-cert.cni.es	2015-12-01	Medium	Completed	Trj/CryptoLocker
				Threat:Ransomware						
✓	Panda	Panda	30759	Panda	7	panda@ccn-cert.cni.es	2015-12-01	Medium	Completed	Win32.Bagsulrfrn
✓	Panda	Panda	30758	Panda	7	panda@ccn-cert.cni.es	2015-12-01	Medium	Completed	Trojan-Dropper.Win32.VB
					6	panda@ccn-cert.cni.es	2015-12-01	Medium	Completed	Trojan-Ransom.Win32.Snocry
					20	panda@ccn-cert.cni.es	2015-12-01	Medium	Completed	Trj/Injector
				Symantec	8	sym@ccn-cert.cni.es	2015-12-01	Medium	Completed	JSocket Phishing Campaign Targets Financial Businesses
				Ransomware	187	ccn-cert@cni.es	2015-12-01	Medium	Ongoing	TeslaCrypt
				CERT						

500 eventos nuevos
todos los meses.

DEMO

Valor diferencial

Federación con organismos internacionales.

Fuentes especialistas en malware.

Variedad de atributos y eventos contextualizados.

Interacción con herramientas de análisis.

Histórico y anotaciones de otros equipos.



➤ E-Mails

- info@ccn-cert.cni.es
- ccn@cni.es
- sondas@ccn-cert.cni.es
- redsara@ccn-cert.cni.es
- organismo.certificacion@cni.es

➤ Websites

- www.ccn.cni.es
- www.ccn-cert.cni.es
- www.oc.ccn.cni.es



Síguenos en Linked in

